Remarks and Arguments

Claims 1-30 have been presented for examination. Claims 1-4, 6-11, 13-14, 16-21, 23-24 and 26-30 have been amended. Claims 5, 15 and 25 have been canceled.

Claims 1-30 have been objected to for a number of informalities. In particular, claims 2-5 have been objected to because they all recite a step (d) which the examiner finds confusing. In response, claim 2 had been amended to recite step (k) in order to conform it to the changes in amended claim 1. Claims 3 and 4 have been amended to eliminate the recitation of an explicit step and claim 5 has been canceled. Accordingly, claims 2-5 are now believed to be clear.

Claim 11 has been amended to change the term "Apparatus" to "An apparatus" as requested. The term "unsecure" recited in claims 1, 9, 10, 19 and 20 has been changed to "unsecured" as requested. Accordingly, claims 1, 9, 10 19 and 20 are believed to be clear.

Claim 2 was also objected to because it recited a "scheduled key" which the examiner found unclear as to whether the recited scheduled key was the same as the "scheduled key" recited in claim 1. Claim 1 has now been amended, in lines 14-15, to recite "...encrypting the distribution archive file with a scheduled key unique to that distribution archive file..." Consequently, it is clear that each scheduled key is unique to the archive file with which it is associated. Therefore, the scheduled key used to decrypt the first archive file recited in claim 2 cannot be the same key as that recited in claim 1 because claim 1 recites that an archive file is decrypted with a scheduled key from a subsequent archive file.

Claims 1-10, 19-20 and 29-30 were rejected under 35 U.S.C. §112, second paragraph, because the examiner considered steps (a)-(c) to form an indefinite loop. In particular, step (a) recited extracting a key from a first archive file step (b) recited decrypting the archive file which follows the first archive file with the extracted key and step (c) recited repeating steps (a) and (b) thus reciting repeatedly extracting the key from the first archive file and decrypting the second archive file.

In response, claim 1 has been amended to recite, in lines 17-24, (f) selecting a file from the stream, (g) extracting a scheduled key from the selected file, (h) using the extracted scheduled key to decrypt the next subsequent file in the stream following the

selected file, (i) removing the encrypted document content and the key pair list from the decrypted distribution archive file and storing them at the unsecured site and (j)

selecting the distribution archive file decrypted in step (h) and repeating steps (g), (h), (i) and (j) for each distribution archive file in the stream. It is believed that claim 1 as amended is clear with respect to the sequence of actions. Claims 2-10 have presumably been rejected for their dependence on claim 1. Accordingly, these latter claims are also believed to particularly point out and distinctly claim the invention as required by 35 U.S.C. §112, second paragraph.

Claims 9, 19 and 29 have been rejected because the examiner claims they recite that encryption of the scheduled key takes place at the unsecured site whereas the parent claims recite that the encryption takes place at the publishing site. Claims 9, 19 and 29 originally incorrectly recited that the scheduled key was encrypted with a text string. Claims 9, 19 and 29 have been amended to recite that the document identifier is encrypted with a text string that has been embedded into program code located at the unsecured site. Claims 7, 17 and 27 have also been amended to correct the original incorrect recitation of a scheduled key. It is believed that these claims, as amended, clearly indicate how the document identifier is computed and recomputed and are thus, in accordance with 35 U.S.C. §112, second paragraph.

Claims 1-30 have been rejected under 35 U.S.C. §102(a) as anticipated by PCT Patent Publication No. WO 2002/100037 (Shen.) The examiner has included citations from a corresponding U.S. Patent Publication No. 2004/0236956 and these will be used in the discussion below. The examiner comments that the reference discloses all of the claimed limitations.

The invention relates to securely providing content in documents from a publishing site to users located at an unsecured site. Rather than downloading each document on demand from the publishing site to the user site, at the publisher location, each document is assigned a document ID and encrypted and then a plurality of encrypted documents are assembled into a distribution archive that is itself encrypted with a "scheduled" key that is created specially for that archive. The distribution archive file also includes a list of document IDs and the decryption keys associated with those document IDs. The distribution archive is then downloaded into a content server at the

user site. When the content server receives the distribution archive, it decrypts the archive file and unpacks the encrypted documents, but does not decrypt each document. Instead, the encrypted documents are stored in encrypted form in a local document database to be later decrypted on demand. The scheduled key to decrypt an archive file is included with an archive file that was sent previously to the user site. This prevents a third party who has improperly obtained the archive file from decrypting the file unless the third party has also obtained a copy of the previous archive file.

Later, when a user wishes to view a document, a viewer in the user's computer re-computes the document ID from the encrypted content in the local content server. Thus, it is important that the document ID cannot be calculated from the encrypted content alone. The document ID is related to the encrypted content, but not directly derivable from that content. In one embodiment, the document ID is re-computed from the encrypted content and a secret text string embedded in the viewer program code. Once the ID has been calculated, it is used to access the ID/decryption key list and retrieve the decryption key that is then used to decrypt the content.

The Shen reference discloses a content protection scheme in which documents are decrypted as they arrive in a text stream. The reference is particularly directed at decryption "tools" that can be downloaded in front of the content or run remotely before the content is downloaded. These tools configure a conventional computer to decrypt content encrypted in a particular format. They allow the computer to receive and decrypt content no matter which encryption format has been used.

However, there is no disclosure in Shen that the encrypted documents are stored at the download site in encrypted form together with document identifiers that are computed for each document using the encrypted document content for that document but which cannot be derived solely from the encrypted content of that document. Claim 1 has been amended by incorporating the limitations of claim 5. Accordingly, claim 5 has been canceled. Amended claim 1 recites, in lines 7-9, that document identifiers that are computed for each document using the encrypted document content for that document but which cannot be derived solely from the encrypted content of that document. In lines 23-24, amended claim 1 recites that encrypted documents and document identifiers that are computed for each document from the encrypted content

are removed from the archive file and stored at the unsecured download site. Neither of these limitations is disclosed in Shen. The examiner points to the content ID disclosed in Shen as corresponding to the recited document ID. While a content ID is disclosed in Shen, there is no disclosure of how it is calculated. Instead, Shen indicates that incoming documents from different sources are grouped by their content IDs (Shen, paragraph [0088]) indicating that the content IDs are related to the type of content (for example, ASCII text or XML) rather than being related to, but not derivable from, the encrypted content as recited. Thus, amended claim 1 patentably distinguishes over the cited reference.

Claims 2-10 are dependent on claim 1 and incorporate the limitations thereof. Consequently, they distinguish over the cited reference in the same manner as claim 1 as discussed above. In addition, these claims recite additional limitations not disclosed or suggested by the Shen reference. For example, amended claim 7 recites that a document identifier is computed using a text string embedded in program code in the publishing site. Amended claim 9 recites that a document identifier is recomputed with a text string embedded in program code located at the unsecured site. Amended claim 10 recites that the text strings recited in claims 7 and 9 are the same. The examiner points to the "license" key disclosed in Shen that is used to decrypt the scrambling key for scrambled content. Applicants note that Shen does disclose two-layer security in which an encryption or decryption key it itself encrypted or decrypted with another key called a "license" key. However, there is no description in Shen that the license key comprises a text string embedded in program code as recited. Consequently, claims 7, 9 and 10 also patentably distinguish over the Shen reference for this reason also.

Claim 11 has been amended in a manner similar to claim 1 by incorporating the limitations of claim 15. Accordingly, claim 15 has been canceled. Since amended claim 11 contains limitation equivalent to amended claim 1, it distinguishes over the cited Shen reference in the same manner as amended claim 1 as discussed above.

Claims 12-20 are dependent on claim 11 and incorporate the limitations thereof. Consequently, they distinguish over the cited reference in the same manner as claim 11 as discussed above. In addition, these claims recite additional limitations not disclosed or suggested by the Shen reference. For example, claims 17, 19 and 20 contain

limitations that parallel those recited in claims 7, 9 and 10. Therefore, they also distinguish over the cited references in the same manner as these latter claims.

Claim 21 has been amended in a manner similar to claim 1 by incorporating the limitations of claim 25. Accordingly, claim 25 has been canceled. Since amended claim 21 contains limitation equivalent to amended claim 1, it distinguishes over the cited Shen reference in the same manner as amended claim 1 as discussed above.

Claims 22-30 are dependent on claim 21 and incorporate the limitations thereof. Consequently, they distinguish over the cited reference in the same manner as claim 21 as discussed above. In addition, these claims recite additional limitations not disclosed or suggested by the Shen reference. For example, claims 27, 29 and 30 contain limitations that parallel those recited in claims 7, 9 and 10. Therefore, they also distinguish over the cited references in the same manner as these latter claims.

In light of the forgoing amendments and remarks, this application is now believed in condition for allowance and a notice of allowance is earnestly solicited. If the examiner has any further questions regarding this amendment, he is invited to call applicants' attorney at the number listed below. The examiner is hereby authorized to charge any fees or direct any payment under 37 C.F.R. §§1.17, 1.16 to Deposit Account number 50-3969.

Respectfully submitted

/paul e. kudirka/ Date: 2007-01-31

Paul E. Kudirka, Esq. Reg. No. 26,931
LAW OFFICES OF PAUL E. KUDIRKA
Customer Number 64967
Tel: (617) 357-0010 Fax: (617) 357-0035